PUBLIC DOMAIN — CC0 1.0 UNIVERSAL — CANNOT BE CLASSIFIED — CANNOT BE SUPPRESSED — CANNOT BE UNWRITTEN

THE HUMAN SOVEREIGNTY TECHNOLOGY PARADIGM

Supplement Version 2.0 — Extended Prior Art Declaration

"Technology Must Serve the Human. Never the Possessor."

PUBLICATION DATE	June 3, 2026
INVENTOR / AUTHOR	Braydon Alexander Kershner — Sole Inventor
PATENT STATUS	US Provisional Application No. 64/020,809 — PATENT PENDING — Filed March 29, 2026 — Non-Provisional in preparation
SUPPLEMENTS	Version 1.0 (March 29, 2026) — Zenodo Record: zenodo.org/records/19323816 — This document extends Version 1.0 and does not modify or replace it. Both documents together constitute the complete prior art record.
PURPOSE	Extend prior art protection to: no-biometric embodiments; third-party wearable compatibility; CEEP electrode architecture; modular replacement architecture; AI federated learning protocol; multi-mode trigger subsystem; passive safe-discharge adapter; extended application embodiments not covered in Version 1.0
LICENSE	CC0 1.0 Universal — Irrevocable Public Domain Dedication — All concepts herein are freely usable by anyone for any lawful purpose. No rights reserved. No attribution required.
ARCHIVES	Zenodo / CERN — zenodo.org | Electronic Frontier Foundation — info@eff.org | Committee to Protect Journalists — info@cpj.org | Freedom of the Press Foundation — info@freedom.press | Reporters Without Borders — dcdesk@rsf.org | American Civil Liberties Union — aclu.org/contact
LEGAL EFFECT	Published prior art under 35 U.S.C. § 102(a)(1) as of June 3, 2026. Cannot be retroactively classified under 35 U.S.C. § 181 after this date.
CONTACT	americanpublication@protonmail.com

LEGAL NOTICE: Published June 3, 2026 as a supplement to Version 1.0 (zenodo.org/records/19323816). All concepts described herein that are not claimed as patentable subject matter are irrevocably dedicated to the public domain under CC0 1.0 Universal. This document constitutes published prior art under 35 U.S.C. § 102(a)(1) and cannot be retroactively classified after this publication date.

PART I — PREAMBLE: WHY THIS SUPPLEMENT IS NECESSARY

Version 1.0 of the Human Sovereignty Technology Paradigm white paper, published March 29, 2026, established irrevocable public domain prior art for the principles, prohibitions, and general application concepts of this platform. That publication occurred simultaneously with the filing of United States Provisional Patent Application No. 64/020,809 and was specifically designed to prevent retroactive government classification of the foundational principles.

This supplement addresses key gaps identified during preparation of the non-provisional patent application. The most significant gaps are addressed in the order of their commercial and legal importance:

- ▶️ Version 1.0 described the platform primarily through the lens of physiological liveness authentication, creating a risk that no-biometric implementations — the broadest and most commercially immediate product tier — were not explicitly established as prior art. This supplement closes that gap completely.
- ▶️ Version 1.0 did not explicitly establish that commercially available third-party wearable devices may serve as the physiological sensing means for the liveness relay protocol. This concept must be prior art to prevent competitors from claiming exclusive rights to this integration approach.
- ▶️ Several specific technical architectures developed during non-provisional preparation — including the CEEP electrode system, the modular replacement architecture with cryptographic authentication, the passive safe-discharge adapter, and the AI federated learning protocol — require explicit public domain dedication.
- ▶️ The weapon authentication embodiment requires additional specificity regarding the unconditional mechanical override mandate and the absolute prohibition on government remote disable capability, to prevent any implementation that circumvents these protections.
- ▶️ The financial system embodiment requires explicit prior art dedication of the coercion detection during payment authorization concept.
- ▶️ The quantum, biological, and neural computing applicability of the operator-bound principle requires explicit prior art dedication to prevent future technology patents from excluding this platform from emerging technology domains.

This supplement does not alter, modify, limit, or supersede the Version 1.0 white paper in any respect. It extends the prior art record. Both documents together constitute the complete public domain dedication of the Human Sovereignty Technology Paradigm.

> **Version 1.0 (March 29, 2026) remains in full force and effect exactly as published. This supplement adds to it. Read both documents together for the complete prior art record.**

PART II — THE NO-BIOMETRIC PRINCIPLE

II.1 The Operator-Bound Technology Principle Is Authentication-Agnostic

The single most important clarification this supplement establishes as prior art is this: the Operator-Bound Technology Principle — technology serving exclusively its designated human operator, storing no data beyond authenticated sessions, and destroying all operator data upon defined trigger conditions — is a design architecture that functions completely and independently of any biometric or physiological authentication component.

Authentication of the operator prior to system access may be accomplished by any means or combination of means, including without limitation: physiological liveness verification of any type; biometric verification of any type; cryptographic credential; personal identification number; password; passphrase; physical proximity token; physical key; possession of an authenticated companion device; challenge-response protocol; knowledge-based authentication; or any combination thereof.

Authentication may also be entirely absent. In configurations where the operative security function is provided entirely by automatic trigger conditions — such as automatic destruction upon tamper detection, media removal, geographic boundary breach, time expiration, or remote command — no active operator authentication is required and the system remains fully within the scope of the Operator-Bound Technology Principle.

This concept — the Operator-Bound Technology Principle operating without any biometric or physiological authentication requirement — is irrevocably dedicated to the public domain under CC0 1.0 as of June 3, 2026. No patent application filed after this date may claim exclusive rights to this concept without limitation to a specific novel implementation not described herein.

II.2 Complete List of Non-Biometric Trigger Means — Public Domain

The following trigger means for data destruction and system sanitization, all operating independently of any biometric or physiological authentication, are hereby irrevocably dedicated to the public domain as of June 3, 2026:

- ✓ Manual actuation of any designated trigger element by the operator — including any button, switch, capacitive touch sensor, pressure sensor, voice command, gesture, eye movement, proximity gesture, or any physical actuation means of any type
- ✓ Automatic detection of unauthorized removal or displacement of storage media from a receiving device or bay without prior authenticated authorization by the operator
- ✓ Receipt of an authenticated remote destruction command via any communication means — including NFC, Bluetooth Low Energy, Bluetooth Classic, WiFi, cellular (2G/3G/4G/5G/6G and beyond), satellite, LoRa, mesh network, ultrasonic, optical, or any present or future wireless communication protocol
- ✓ Expiration of a configurable time-based session limit without authenticated renewal within the configured interval
- ✓ Detection of communication bus patterns, software enumeration sequences, or filesystem access patterns consistent with forensic examination tools, unauthorized system interrogation, or data exfiltration attempts
- ✓ Detection of electromagnetic scanning, X-ray exposure, terahertz imaging, neutron radiography, or any non-contact interrogation technology applied to the device or its contents
- ✓ Detection of unauthorized physical access to, tampering with, or disassembly of a device enclosure — including vibration, pressure, light exposure, continuity interruption, or any other tamper-evident means
- ✓ Detection of acoustic trigger patterns, voice commands, voice prints, or ultrasonic signals designated by the operator as destruction triggers

- ✓ Detection of proximity of any designated threat indicator including electronic surveillance devices, signal jammers, unauthorized RFID readers, stingrays or IMSI catchers, or any device the operator designates as a threat indicator
- ✓ AI-autonomous determination that threat probability exceeds a configurable threshold based on fusion of any available sensor inputs with no network connectivity requirement
- ✓ Geographic boundary breach — when device location moves outside a configurable geofence without prior authenticated override
- ✓ Detection of removal of a designated companion device — such as a paired wearable — beyond configurable signal range or signal cessation beyond configurable duration
- ✓ Power removal or battery depletion beyond a configurable threshold without prior authenticated suspend command
- ✓ Detection of connection to any unauthorized host system, network, or charging source not on an operator-approved list
- ✓ Any logical OR, AND, or weighted combination of any of the above trigger conditions

Any device, system, method, or protocol that destroys, sanitizes, or renders irrecoverable any operator data in response to any one or more of the above trigger means, without requiring biometric authentication as a necessary condition of operation, is within the scope of this prior art dedication as of June 3, 2026.

II.3 Non-Biometric Product Embodiments — Public Domain

The following specific product and system embodiments implementing the Operator-Bound Technology Principle without biometric authentication are irrevocably dedicated to the public domain as of June 3, 2026:

Portable External Data Destruction Device

A portable, person-carried device containing an onboard rechargeable energy source, high-voltage generation means, primary energy storage element, one or more receiving bays accepting any digital storage interface, pre-positioned internal electrodes contacting inserted media semiconductor dies, two-stage manual trigger means, automatic trigger means responding to any condition described in Part II.2, post-discharge energy absorption means, and safe discharge pathway — that destroys inserted storage media by delivering destructive electrical energy through said pre-positioned electrodes, without network connectivity, external power, or biometric authentication, in a form factor suitable for keychain or pocket carry.

No-Storage Computing Terminal

A computing device containing no persistent internal storage of any kind by design, booting exclusively from storage presented by a connected operator device authenticated by cryptographic challenge-response, with all session data stored exclusively in volatile memory, and providing cryptographically verified attestation of complete data purge upon each session termination — without biometric authentication requirement.

No-Biometric Vehicle Authentication System

A vehicle operation authorization system requiring a connected authenticated operator device for all vehicle operation, storing all operator preferences exclusively in volatile vehicle memory during authenticated sessions, purging all operator data from all vehicle systems upon session termination by any means, and

enabling temporary scoped operational authority delegation to secondary operator devices — without biometric authentication of the primary or secondary operator.

Universal Session Data Impermanence Protocol

A protocol applied to any host system — including vehicles, hotels, computing terminals, medical facilities, financial systems, electoral systems, rental systems, and any other system — requiring volatile-only storage of all operator data during sessions and cryptographically verified complete purge upon session termination, without biometric authentication.

Non-Biometric Selective Destruction System

A zoned data destruction system with user-defined threat profiles mapping trigger conditions to destruction scope across independently addressable data containers, with per-container independent destruction means, operable by manual trigger or automatic condition detection, without biometric authentication.

Passive Safe-Discharge Adapter

A passive adapter device enabling safe dissipation of residual electrical energy from a data destruction device through: (a) any standard building electrical outlet by connection to the neutral conductor through a current-limiting element; (b) a conductive soil probe insertable into any soil or sand; or (c) any vehicle chassis or equipment rack ground point — without requiring active power, network connectivity, electronic circuitry, or operator expertise beyond physical insertion.

Modular Replacement Architecture

A data security device architecture comprising a permanent chassis and interchangeable functional modules secured by a proprietary connector, wherein each module contains a cryptographic authentication element verified by the chassis before acceptance, modules consumed by destruction events are replaceable enabling device reuse, and each destruction event generates a recurring module replacement transaction independent of new chassis sales — creating a razor-and-blade recurring revenue model built into the device architecture.

PART III — THIRD-PARTY WEARABLE COMPATIBILITY

III.1 The Wearable Liveness Relay Protocol — Any Device Compatible

The following concept is irrevocably dedicated to the public domain as of June 3, 2026: a liveness relay protocol in which any wearable or implanted device providing continuous physiological data — including any commercially available third-party device — serves as the physiological sensing means for an operator-bound technology system, transmitting continuous vital sign status to a connected operator device via any wireless communication protocol, enabling the operator device to maintain operator liveness confirmation and trigger defined responses upon signal cessation or vital sign absence beyond a configurable threshold.

The following specific third-party device categories and implementations are explicitly prior art as of June 3, 2026:

- ✓ Any Apple Watch model or future Apple wearable device providing continuous cardiac, ECG, PPG, SpO2, or any physiological data via HealthKit, CoreMotion, or any Apple API or wireless protocol
- ✓ Any Samsung Galaxy Watch model or future Samsung wearable device providing continuous cardiac, ECG, PPG, or physiological data via Samsung Health SDK, Samsung BioActive sensor API, or any Samsung API or wireless protocol
- ✓ Any Garmin wearable device providing continuous heart rate, HRV, SpO2, or physiological data via Garmin Health API, Connect IQ SDK, or any Garmin API or wireless protocol
- ✓ Any Fitbit, Google Pixel Watch, or Google wearable device providing continuous cardiac or physiological data via Google Health Connect, Fitbit Web API, or any Google API or wireless protocol
- ✓ Any Oura Ring model or future smart ring device of any form factor providing continuous physiological monitoring via Oura API or any wireless protocol
- ✓ Any Whoop, Polar, Suunto, Withings, Amazfit, Huawei Watch, or any other wearable device of any manufacturer providing continuous physiological data via any API or wireless protocol
- ✓ Any FDA-cleared or CE-marked medical monitoring wearable of any type providing continuous cardiac, neurological, respiratory, or other physiological data
- ✓ Any implanted device including pacemakers, neurostimulators, continuous glucose monitors, or any implanted sensor providing continuous physiological data to external systems via any wireless communication means
- ✓ Any future wearable or implanted device of any form factor providing any physiological monitoring data via any communication means — present or future

The inventive contribution of the operator-bound technology platform is the liveness relay protocol and its integration with the destruction and succession systems. The physiological sensor hardware itself is not the inventive contribution. Third-party devices serving as the physiological sensor are within the scope of this prior art dedication and cannot be claimed exclusively by any party as the sensing means in an operator-bound technology liveness relay system.

III.2 Proprietary Wearable Line — Also Prior Art

The concept of a proprietary wearable monitoring device specifically designed for integration with the operator-bound technology platform, providing enhanced security features including cryptographically authenticated data transmission, tamper detection, anti-removal detection, and anti-spoofing measures beyond those available in commercial devices, is also dedicated to the public domain as of June 3, 2026 as an application concept. The specific implementation details of any proprietary wearable line may be the subject of separate patent protection.

PART IV — TECHNICAL ARCHITECTURE PRIOR ART

IV.1 CEEP Electrode Architecture

The Capacitive Energy Entry Point (CEEP) electrode architecture is irrevocably dedicated to the public domain as of June 3, 2026. CEEP comprises: conductive electrode elements manufactured into or permanently positioned within a storage media interface module; positioned in direct physical proximity to and electrical contact with target semiconductor die components of any inserted storage device; configured to receive and

deliver destructive electrical energy — from any capacitive, inductive, or stored energy source — directly to said semiconductor dies through conductive contact without requiring any mechanical deployment, penetrating element, chemical agent, or explosive material. The result is permanent and forensically irrecoverable destruction of all data stored in said semiconductor components.

Key properties of the CEEP architecture that are prior art as of June 3, 2026:

- ✓ Pre-positioning at manufacturing time — no mechanical deployment required during destruction event
- ✓ Direct die contact through electrical interface — energy delivered through the same conductors that normally carry data signals
- ✓ Airline-safe by design — no explosive, incendiary, pressurized, or mechanically deployed components
- ✓ Form factor agnostic — implementable in any receiving bay accepting any storage interface standard
- ✓ Compatible with any energy source capable of generating sufficient voltage and current to cause gate oxide rupture, tunnel oxide breakdown, or bond wire failure in target semiconductor devices
- ✓ Operable without network connectivity, external power, or third-party cooperation

IV.2 AI Threat Assessment and Federated Learning Protocol

The following AI system concept is dedicated to the public domain as of June 3, 2026: an on-device artificial intelligence subsystem executing all security inference exclusively on processing means within the device without requiring network connectivity, providing continuous threat probability scoring from fusion of all available sensor inputs, executing graduated automated responses proportional to threat score, and updating threat models through a federated learning protocol that shares only aggregated model parameter updates across the device population without transmitting any raw sensor data, behavioral data, or identifying information from any individual device.

The graduated response tiers — monitoring only at low threat scores, progressive alerts at intermediate scores, pre-charge of destruction energy at high scores, and autonomous destruction execution at maximum scores — are prior art as of June 3, 2026 in the context of data security devices.

IV.3 Cryptographic Module Authentication for Recurring Revenue

The following business model implementation is dedicated to the public domain as of June 3, 2026: a hardware security device in which each consumable or replaceable module contains a cryptographic authentication element that the device chassis verifies before accepting the module for use, wherein counterfeit or unauthorized modules are cryptographically rejected, generating a recurring authenticated replacement module revenue stream following each destruction event.

IV.4 Networked Remote Destruction Coordination

The concept of coordinated authenticated remote destruction commands delivered via any communication means to any number of registered devices simultaneously or sequentially, enabling an authorized administrator to remotely sanitize any or all registered devices from any location with network or communication access, is dedicated to the public domain as of June 3, 2026.

IV.5 Future Technology Applicability

The Operator-Bound Technology Principle and all associated subsystems described in Version 1.0 and this supplement apply without limitation to all present and future technology including: quantum computing systems; quantum communication systems; biological computing systems; synthetic biological systems; neural dust and distributed neural interface systems; brain-computer communication systems of any type; DNA-based storage systems; photonic computing systems; and any technology not yet conceived that authenticates human identity, controls system access, or stores, processes, or transmits information on behalf of a human operator. The application of the Operator-Bound Technology Principle to all present and future technology is prior art as of June 3, 2026.

PART V — EXTENDED APPLICATION EMBODIMENTS — PRIOR ART

V.1 Financial System Embodiment — Extended

The following financial system concepts are dedicated to the public domain as of June 3, 2026, extending the financial application concepts in Version 1.0:

- ✓ Detection of physiological stress indicators consistent with coercion during payment authorization, triggering protective protocols including transaction denial, alert transmission, or silent transaction recording for later reporting
- ✓ Cryptographic succession preventing posthumous access to financial accounts, digital assets, digital currency wallets, or any financial credentials, with automatic transfer of access authority to designated successors upon verified operator incapacitation or death
- ✓ Operator-carried payment credentials never transmitted to or stored in any merchant, payment processor, or financial intermediary system — binary authorization only
- ✓ Zero operator financial data recoverable from any point-of-sale, ATM, banking terminal, or financial system following transaction completion

V.2 Weapon Authentication — Extended and Strengthened

The following weapon authentication concepts are dedicated to the public domain as of June 3, 2026, extending the Second Amendment Preservation Provision of Version 1.0 with greater specificity:

- ✓ Unconditional mechanical override means that completely bypasses all electronic authentication systems and returns any weapon to fully mechanical operation identical to its pre-electronic-modification function, operable by the weapon owner in the field without tools, codes, credentials, network connectivity, or external assistance of any kind
- ✓ Electronic authentication as an additive security layer only — never as a dependency of the weapon's primary mechanical function under any circumstances
- ✓ Absolute architectural prohibition of any remote disable, restrict, or command capability accessible by any party other than the authenticated weapon owner
- ✓ Absolute prohibition of any network dependency — weapon operability must never depend on any external server, cloud service, government system, or communication link not exclusively controlled by the weapon owner
- ✓ Automatic re-enablement of full mechanical operation if any network dependency, external authorization requirement, or remote command capability is detected in the electronic system

✓ No government, manufacturer, law enforcement, or any other party possesses any master key, override code, or disable capability for any weapon implementing this system

Any implementation of weapon authentication technology that enables remote disabling, government override, network-dependent operability, or any capability reducing the weapon owner's exclusive control is expressly prohibited in any license under the Human Sovereignty Technology Platform patent and is additionally dedicated to the public domain as a prohibited application concept, ensuring it cannot be exclusively patented by any party.

V.3 Child Protection Embodiment — Extended

The following child protection concepts are dedicated to the public domain as of June 3, 2026, extending Version 1.0:

✓ Guardian-authorized monitoring operating exclusively within parameters explicitly set by the legal guardian, with the monitored person informed of all monitoring functions active at any time

✓ No government child monitoring database — all monitoring data stored exclusively on guardian-controlled devices

✓ Automatic complete data deletion and full control transfer to the protected person upon their reaching legal majority in the applicable jurisdiction — no exceptions, no delays, no required action by the former guardian

✓ All monitoring functions terminable at any time by the monitored person once they reach legal majority, with cryptographic proof of termination

✓ Absolute prohibition of child monitoring data sale to any third party under any circumstances

V.4 Medical and Healthcare Embodiment — Prior Art

The following medical system concepts are dedicated to the public domain as of June 3, 2026:

✓ Patient operator device as the exclusive source of all patient identity credentials, medical record access keys, and treatment authorization — no hospital, clinic, or medical provider retains patient identity data following session end

✓ Complete purge of all patient data from any medical device, terminal, or system upon patient session termination, with cryptographically verified attestation

✓ Patient-controlled medical record destruction — the patient operator device holds the exclusive key to all medical records and has the right to irreversibly destroy those records at any time as an expression of medical privacy

✓ No posthumous access to medical records without cryptographic succession authorization from a designated successor designated by the patient prior to incapacitation

V.5 Journalism and Legal Profession Embodiment — Prior Art

The following source protection and legal privilege concepts are dedicated to the public domain as of June 3, 2026:

✓ Zero-knowledge source protection architecture — journalist operator device holds all source identity credentials in encrypted form; no record of source identity exists in any system the journalist does not exclusively control

✓ Emergency source identity destruction — a single trigger action simultaneously destroys all source identity credentials across all connected devices, leaving no recoverable record by any forensic means

✓ Attorney-client privilege protection through architectural impossibility of disclosure — privileged communications stored exclusively on attorney operator device with destruction capability that the attorney can exercise before any compelled disclosure

✓ Duress-triggered silent destruction — destruction of source or client identity data appearing to any observing adversary as normal authentication failure, revealing no indication that destruction occurred

PART VI — EXTENDED PROHIBITIONS — TYRANNICAL APPLICATIONS

The following tyrannical application concepts are irrevocably dedicated to the public domain as of June 3, 2026, not for the purpose of enabling them but to ensure they cannot be exclusively patented — establishing prior art for all such applications so that no party can claim a legal monopoly on any technology implementing them. This prior art dedication additionally serves as notice to any party implementing such applications that they do so in the full public knowledge that these applications exist and have been specifically identified as contrary to individual human freedom and dignity.

✗ Use of operator-bound authentication technology to implement government-controlled weapon disable infrastructure — any system in which weapon operability depends on government, military, or law enforcement authorization signals

✗ Use of physiological authentication data collected under the operator-bound technology protocol to build behavioral profiles of individuals without their specific, informed, ongoing, and revocable consent

✗ Use of session data impermanence architecture to evade legal data preservation obligations that arose before the session in question — impermanence is a forward-looking privacy protection, not a tool for destroying evidence of past conduct

✗ Use of modular replacement architecture to implement mandatory government-controlled module authentication — any system where replacement modules require government approval for civilian use

✗ Use of wearable liveness relay protocol data to track operator location, activity patterns, or behavioral characteristics for any purpose other than liveness confirmation and destruction triggering

✗ Use of federated learning to aggregate behavioral patterns from individual users to enable population-level surveillance, behavioral prediction, or social scoring

✗ Use of AI threat assessment to implement employer behavioral scoring, government citizen monitoring, or insurance company health discrimination

✗ Use of no-storage terminal architecture to implement systems that appear to respect privacy while secretly exfiltrating data before the session purge

✗ Use of voter verification architecture to create any record of which candidate or measure a voter voted for, by any technical means including timing analysis, network traffic analysis, or inference

✗ Use of child protection monitoring beyond the age of legal majority under any circumstances, for any reason, by any party

- ✗ Use of cryptographic succession protocol to enable automatic inheritance of digital assets by governments, corporations, or any party other than the operator-designated human successors
- ✗ Use of emergency data destruction capability by any party other than the operator themselves — no government, court, employer, or other party may trigger destruction of operator data without the operator's prior explicit consent

PART VII — CONSTITUTIONAL AND HUMAN RIGHTS FRAMEWORK — EXTENDED

All constitutional and human rights provisions established in Version 1.0 apply equally to all concepts described in this supplement. The following additional constitutional and human rights principles are established as part of the Human Sovereignty Technology Paradigm framework as of June 3, 2026:

The Right to Digital Silence

Just as individuals have a constitutional right against compelled self-incrimination under the Fifth Amendment to the United States Constitution and equivalent provisions of all constitutional democracies, individuals have a corresponding right to destroy their own digital records as an act of conscience, self-protection, or legal defense, provided such destruction does not occur in violation of a specific, lawfully issued, and judicially reviewed preservation order. The technology described in this platform implements this right in hardware. No license under any patent covering this technology may be used to undermine this right.

The Right to Technological Self-Determination

Every person has the right to determine the terms under which technology operates in their life — including the right to define what data is collected, how long it is retained, who may access it, and under what conditions it is destroyed. Technology that overrides this right without specific, informed, ongoing, and revocable consent violates human dignity regardless of its legality under any particular jurisdiction's laws. This platform is designed to implement technological self-determination as a default rather than an exception.

Individual Conscience Protection — Nuremberg Principle IV Implementation

No military, law enforcement, or governmental implementation of this technology shall prevent any individual operator from rendering their own credentials and connected systems inoperable as an act of conscience, including when the operator believes they have been ordered to commit an act contrary to international humanitarian law, the laws of armed conflict, or fundamental human rights. The individual operator's right to destroy their own credentials rather than comply with an unlawful order is absolute, unconditional, and technologically protected by this platform. This provision implements Nuremberg Principle IV — that individuals have a duty to refuse unlawful orders — in operational technology.

PART VIII — ANTI-SUPPRESSION ARCHITECTURE

This supplement has been simultaneously submitted for permanent archiving to all organizations listed in the metadata table above. The multi-organizational, multi-jurisdictional archiving strategy is designed to ensure that no single point of failure — technical, legal, or political — can result in suppression of this document.

Zenodo (CERN), located in Geneva, Switzerland, operates under Swiss law and European Union regulations. It is beyond the legal jurisdiction of the United States government for purposes of document suppression. Its permanent DOI system ensures this document remains permanently accessible regardless of any action taken in any US court.

The civil liberties organizations listed as archives — the Electronic Frontier Foundation, Committee to Protect Journalists, Freedom of the Press Foundation, Reporters Without Borders, and American Civil Liberties Union — each have institutional mandates to resist government suppression of published information. Their receipt and archiving of this document creates an independent public record held by organizations specifically designed to publicize suppression attempts.

Under 35 U.S.C. § 181, a Secrecy Order may be imposed on a patent application during prosecution if the USPTO determines it has national security implications. A Secrecy Order applies to the patent application — not to independently published prior art. This document, published before any Secrecy Order could be issued, is not subject to Secrecy Order restriction. Its publication date of June 3, 2026 is established and immutable. Any Secrecy Order issued after this date cannot affect the public domain status of the concepts described herein.

Under 28 U.S.C. § 1498, if the US government uses an invention covered by a granted patent without license, the patent owner's exclusive remedy is just compensation in the US Court of Federal Claims. The inventor retains ownership. The government does not acquire the patent. The inventor retains the right to license the patent commercially in all non-government applications. The public white paper record established by Versions 1.0 and 2.0 of this document ensures that the principles underlying the platform remain in the public domain regardless of what happens to the patent during prosecution.

CANNOT BE CLASSIFIED. CANNOT BE SUPPRESSED. CANNOT BE RETROACTIVELY RESTRICTED. CANNOT BE UNWRITTEN. Published: June 3, 2026. Archived internationally. Witnessed permanently.

[END — THE HUMAN SOVEREIGNTY TECHNOLOGY PARADIGM — SUPPLEMENT VERSION 2.0]

Published: June 3, 2026 | Inventor: Braydon Alexander Kershner | License: CC0 1.0 Universal
Patent Pending — USPTO Provisional Application No. 64/020,809 — Filed March 29, 2026